The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
9/28/2011

SUBJECT:
Multiple Vulnerabilities in Mozilla Products Could Allow Remote Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Mozilla Firefox, Thunderbird, and SeaMonkey applications, which could allow remote code execution. Mozilla Firefox is a web browser used to access the Internet. Mozilla Thunderbird is an email client. Mozilla SeaMonkey is a cross platform Internet suite of toolsranging from a web browser to an email client.

These vulnerabilities may be exploited if a user visits, or is redirected to a specially crafted web page. Successful exploitation of these vulnerabilities will result in either an attacker gaining the same privileges as the logged on user, or gaining session authentication credentials. Depending on the privileges associated with the user, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:
- Mozilla Firefox prior to 3.6.20
- Mozilla Firefox prior to 6.0
- Mozilla Sea Monkey prior to 2.4
- Mozilla Thunderbird prior to 3.1.12
- Mozilla Thunderbird prior to 6.0

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

DESCRIPTION:
Multiple vulnerabilities have been discovered in Mozilla Firefox, Thunderbird, and Sea Monkey. Details of these vulnerabilities are as follows:

Mozilla developers identified and fixed several memory safety bugs in the browser engine used in Firefox and other Mozilla-based products. Some of these bugs showed evidence of memory corruption under certain circumstances, and with enough effort at least some of these could be exploited to run arbitrary code. This issue affects Firefox 3.6.23 and 6. (CVE-2011-2995, CVE-2011-2996, CVE-2011-2997)

Firefox is prone to a remote integer-underflow vulnerability because it fails to sufficiently validate an integer value. The vulnerability occurs when the application handles a specially crafted and overly large JavaScript RegExp expression. This issue affects Firefox 3.6.23.

A XSS vulnerability was discovered where a frame named "location" could shadow the window.location object unless a script in a page grabbed a reference to the true object before the frame was created. Because some plugins use the value of window.location to determine the page origin, this could fool the plugin into granting the plugin content access to another site or the local file system in violation of the Same Origin Policy. This flaw allows circumvention of the fix added for MFSA 2010-10. This issue affects Firefox 3.6.23 and 6, Thunderbird 6, SeaMonkey 2.3. (CVE-2011-2999)

A possible CRLF condition exists when multiple Location headers were present in a redirect response. Mozilla has also corrected the headers Content-Length and Content-Disposition. This issue affects Firefox, Thunderbird and SeaMonkey. (CVE-2011-3000)

If a user hold downs the Enter key, a malicious page could pop up a download dialog where the held key would then activate the default Open action. It is also reported a similar flaw with manual plugin installation using the PLUGINSPAGE attribute. This issue affects Firefox, Thunderbird and SeaMonkey. (CVE-2011-2372, CVE-2011-3001)

In the ANGLE library used by WebGL, the return value from GrowAtomTable() was not checked for errors. If an attacker could causerequests that exceeded the available memory, those would fail and potentially lead to a buffer overrun. This issue affects Firefox and SeaMonkey. (CVE-2011-3002, CVE-2011-3003)

A potentially exploitable crash in the YARR regular expression library used by JavaScript. This issue affects Firefox, Thunderbird and SeaMonkey. (CVE-2011-3232)

The JSSubScriptLoader "unwraps" XPCNativeWrappers when they were used as the scope parameter to loadSubScript(). Without the protection of the wrappers the add-on could bevulnerable to privilege escalation attacks from malicious web content. Thisissue affects Firefox 3.6 and earlier, SeaMonkey 2.3 (CVE-2011-3004)

When loading a specially crafted .ogg file Firefox crashes. This is due to a use-after-free condition and could potentially beexploited to install malware. (CVE-2001-3005)

A limit has been placed on motion data events to the currently-active tab to prevent the possibility of background tabs attempting to decipher keystrokes the user is entering into the foreground tab.

These vulnerabilities may be exploited if a user visits, or is redirected to a specially crafted web page. Successful exploitation of these vulnerabilities will result in either an attacker gaining the same privileges as the logged on user, or gaining session authentication credentials. Depending on the privileges associated with the user, an attacker could install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:

The following actions should be taken:

- Upgrade vulnerable Mozilla products immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

REFERENCES:

Mozilla:

http://www.mozilla.org/security/announce/2011/mfsa2011-36.html

http://www.mozilla.org/security/announce/2011/mfsa2011-37.html
http://www.mozilla.org/security/announce/2011/mfsa2011-38.html
http://www.mozilla.org/security/announce/2011/mfsa2011-39.html
http://www.mozilla.org/security/announce/2011/mfsa2011-40.html
http://www.mozilla.org/security/announce/2011/mfsa2011-41.html
http://www.mozilla.org/security/announce/2011/mfsa2011-42.html
http://www.mozilla.org/security/announce/2011/mfsa2011-43.html
http://www.mozilla.org/security/announce/2011/mfsa2011-44.html
http://www.mozilla.org/security/announce/2011/mfsa2011-45.html

Security Focus:
http://www.securityfocus.com/bid/49800
http://www.securityfocus.com/bid/49808
http://www.securityfocus.com/bid/49809
http://www.securityfocus.com/bid/49810
http://www.securityfocus.com/bid/49812
http://www.securityfocus.com/bid/49813

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2372
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2995
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2996
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2997
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2999
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3000
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3001
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3002
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3003
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3232